AMENDMENTS TO THE CLAIMS:

Please amend claims 1-10, 13-15, 17-20, 22-24 and 27 as follows.

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A ~~computer program product~~program stored on a computer-readable medium for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers, said computer program product comprising:

receiving code ~~operable to receive~~for receiving at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting code ~~operable to detect~~for detecting from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching ~~one or more~~at least one predetermined trigger patterns; and

action performing code ~~operable in response~~, responsive to detection of one ~~or more~~of said at least one predetermined trigger patterns to perform at least one ~~or more~~ predetermined anti-malware actions.

2. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 1, wherein said plurality of network connected computers

each have a malware scanner ~~that serves to scan~~for scanning computer files to detect~~ed~~ malware within said computer files.

3. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 2, wherein said malware scanner ~~uses~~includes malware definition data ~~to identify~~for identifying malware to be detected.

4. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 3, wherein said at least one ~~or more~~ predetermined anti-malware action~~s~~ include~~s~~ forcing an update of malware definition data being used by one or more of said plurality of network connected computers.

5. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 2, wherein said at least one ~~or more~~ predetermined anti-malware action~~s~~ include~~s~~ altering at least one scanner setting of at least one of said malware scanner~~s~~ such that said at least one of said malware scanner~~s~~ performs more thorough malware scanning.

6. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 1, wherein said at least one ~~or more~~ predetermined anti-malware action~~s~~ include~~s~~ isolating at least one ~~of more~~ of said network connected computers from other parts of said computer network.

7. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 1, wherein said managing computer stores said plurality of log data messages within a database.

8. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 7, wherein said detecting code is operable to query said database.

9. (currently amended) A ~~computer program product~~program stored on a computer-readable medium as claimed in claim 7, wherein said database includes data identifying at least one ~~or more~~ of:

malware protection mechanisms used by respective network connected computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.

10. (currently amended) A method of managing malware protection within a computer network containing a plurality of network connected computers, said method comprising the steps of:

receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching at least one ~~or more~~ predetermined trigger patterns; and

in response to detection of said at least one ~~or more~~ predetermined trigger patterns, performing at least one ~~or more~~ predetermined anti-malware actions.

11. (original) A method as claimed in claim 10, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files.

12. (original) A method as claimed in claim 11, wherein said malware scanner uses malware definition data to identify malware to be detected.

13. (currently amended) A method as claimed in claim 12, wherein said at least one ~~or more~~ predetermined anti-malware actions includes forcing an update of malware definition data being used by at least one ~~or more~~ of said plurality of network connected computers.

14. (currently amended) A method as claimed in claim 11, wherein said at least one ~~or more~~ predetermined anti-malware actions includes altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning.

15. (currently amended) A method as claimed in claim 10, wherein said at least one ~~or more~~ predetermined anti-malware actions includes isolating at least one ~~of more~~ of said network connected computers from other parts of said computer network.

16. (original) A method as claimed in claim 10, wherein said managing computer stores said plurality of log data messages within a database.

17. (currently amended) A method as claimed in claim 16, wherein said detecting step includes querying said database.

18. (currently amended) A method as claimed in claim 16, wherein said database includes data identifying at least one ~~or more~~ of:

malware protection mechanisms used by respective network connected computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.

19. (currently amended) Apparatus for managing malware protection within a computer network said computer network containing a plurality of network connected computers, said apparatus comprising:

receiving logic ~~operable to receive~~for receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting logic for detecting~~operable to detect~~ from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching at least one ~~or more~~ predetermined trigger patterns; and

action performing logic ~~operable~~, in response to detection of at least one ~~or more~~ predetermined trigger patterns ~~to perform~~, for performing at least one ~~or more~~ predetermined anti-malware actions.

20. (currently amended) Apparatus as claimed in claim 19, wherein each of said plurality of network connected computers ~~each~~ have a malware scanner that serves to scan computer files to detected malware within said computer files.

21. (currently amended) Apparatus as claimed in claim 20, wherein said malware scanner includes~~uses~~ malware definition data to identify malware to be detected.

22. (currently amended) Apparatus as claimed in claim 21, wherein said at least one ~~or more~~ predetermined anti-malware actions includes forcing an update of malware definition data ~~being used by~~in at least one ~~or more~~ of said plurality of network connected computers.

23. (currently amended) Apparatus as claimed in claim 20, wherein said at least one ~~or more~~ predetermined anti-malware actions includes altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning.

24. (currently amended) Apparatus as claimed in claim 19, wherein said at least one ~~or more~~ predetermined anti-malware actions includes isolating at least one ~~of more~~ of said network connected computers from other parts of said computer network.

25. (original) Apparatus as claimed in claim 19, wherein said managing computer stores said plurality of log data messages within a database.

26. (original) Apparatus as claimed in claim 25, wherein said detecting logic is operable to query said database.

27. (currently amended) Apparatus as claimed in claim 25, wherein said database includes data identifying at least one ~~or more~~ of:

malware protection mechanisms used by respective network connected computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.